

**Escuela Colombiana De Ingeniería
Julio Garavito**

Seguridad y privacidad TI

Daniel Esteban Vela Lopez

Andrés Felipe Montes

Laura Valentina Rodríguez Ortegón

Laboratorio No.10

2024-2

- Integra SonarCloud y Snyk en un repositorio de código de uno de tus proyectos.
- SonarCloud

Después de integrar el repositorio “Lab04_Arsw” en SonarCloud podemos observar que hay 8 vulnerabilidades por corregir. posteriormente también le integramos snyk.

The top screenshot displays the SonarCloud 'Main Branch Summary' for project 'ARSW_Lab4'. The Quality Gate status is 'Not computed'. The summary shows 0 Open Issues, 2 Open Issues, 8 Open Issues, 0 Accepted Issues, 0.0% Coverage, and 0 Duplications. The bottom screenshot shows the 'Issues' page, listing 8 issues with details on their severity, effort, and location in the code.

Issue	Severity	Effort	Location
Intentionality	Major	5min	src/_arsw/blueprints/persistence/BlueprintsPersistence.java
Intentionality	Minor	2min	src/_arsw/blueprints/persistence/impl/Tuple.java
Consistency	Major	5min	src/_arsw/blueprints/services/BlueprintsServices.java
Consistency	Major	5min	src/_arsw/blueprints/services/BlueprintsServices.java
Consistency	Minor	10min	src/_arsw/blueprints/services/BlueprintsServices.java

Snyk

El cual se encargó de corregir algunos de estos errores y se abrió un PR al lab04_Arsw con los cambios realizados.

ORGANIZACIÓN

La Lara

Panel

Proyectos

Integraciones

Miembros

Ajustes

Actualizaciones de produ
Ayuda
lauraortegon7@g...

La Lara > Arreglar > 09a66467 801f 41a1 8d26 5a167a07ed29

Open a Fix PR

lalaro/ARSW_Lab4:pom.xml

Back to project

Issues with a fix

An upgrade is available to fix these issues:

☒

H

Path Traversal In org.springframework:spring-webmvc

☒

L

Improper Handling of Case Sensitivity in org.springframework:spring-context

☒

L

Improper Handling of Case Sensitivity in org.springframework:spring-core

☒

L

Improper Handling of Case Sensitivity in org.springframework:spring-web

☒

L

Improper Handling of Case Sensitivity in org.springframework:spring-webmvc

Open a PR with upgrades and patches to address the selected issues.

Open a Fix PR

lalaro / ARSW_Lab4

Q Type [] to search

+ - 🔍 📧

Code

Pull requests

Actions

Projects

Wiki

Security

Insights

Settings

[Snyk] Fix for 5 vulnerabilities #3

Edit <> Code

Open

lalaro wants to merge 1 commit into master from snyk:fix-8799fc9a167d8c71c2674a5b68c1e62

Conversation

Commits

Checks

Files changed

lalaro commented 3 days ago

Owner

Developer loved, security trusted

Snyk has created this PR to fix 5 vulnerabilities in the maven dependencies of this project.

Snyk changed the following file(s):

- pom.xml

Vulnerabilities that will be fixed with an upgrade:

	Issue	Score	Upgrade
H	Path Traversal SNYK-JAVA-ORGSRINGFRAMEWORK-8230373	721	org.springframework.boot:spring-boot-starter-web: 3.2.10 -> 3.2.11 No Known Exploit
L	Improper Handling of Case Sensitivity SNYK-JAVA-ORGSRINGFRAMEWORK-8230364	401	org.springframework.boot:spring-boot-starter-data-jpa: 3.2.10 -> 3.2.11 org.springframework.boot:spring-boot-starter-web: 3.2.10 -> 3.2.11 No Known Exploit

Reviewers

No reviews

Still in progress? Convert to draft

Assignees

No one—[sign yourself](#)

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

	SNYK-JAVA-ORGSRINGFRAMEWORK-8230372	No Known Exploit
L	Improper Handling of Case Sensitivity SNYK-JAVA-ORGSRINGFRAMEWORK-8230364	401 org.springframework.boot:spring-boot-starter-data-jpa: 3.2.10 -> 3.2.11 org.springframework.boot:spring-boot-starter-web: 3.2.10 -> 3.2.11 No Known Exploit
L	Improper Handling of Case Sensitivity SNYK-JAVA-ORGSRINGFRAMEWORK-8230365	401 org.springframework.boot:spring-boot-starter-data-jpa: 3.2.10 -> 3.2.11 org.springframework.boot:spring-boot-starter-web: 3.2.10 -> 3.2.11 No Known Exploit
L	Improper Handling of Case Sensitivity SNYK-JAVA-ORGSRINGFRAMEWORK-8230366	401 org.springframework.boot:spring-boot-starter-web: 3.2.10 -> 3.2.11 No Known Exploit
L	Improper Handling of Case Sensitivity SNYK-JAVA-ORGSRINGFRAMEWORK-8230368	401 org.springframework.boot:spring-boot-starter-web: 3.2.10 -> 3.2.11 No Known Exploit

Important

- Check the changes in this PR to ensure they won't cause issues with your project.
- Max score is 1000. Note that the real score may have changed since the PR was raised.
- This PR was automatically created by Snyk using the credentials of a real user.

Note: You are seeing this because you or someone else with access to this repository has authorized Snyk to open fix PRs.

For more information:

- [View latest project report](#)
- [Customise PR templates](#)
- [Adjust project settings](#)
- [Read about Snyk's upgrade logic](#)

Development

Successfully merging this pull request may close these issues.

None yet

Notifications

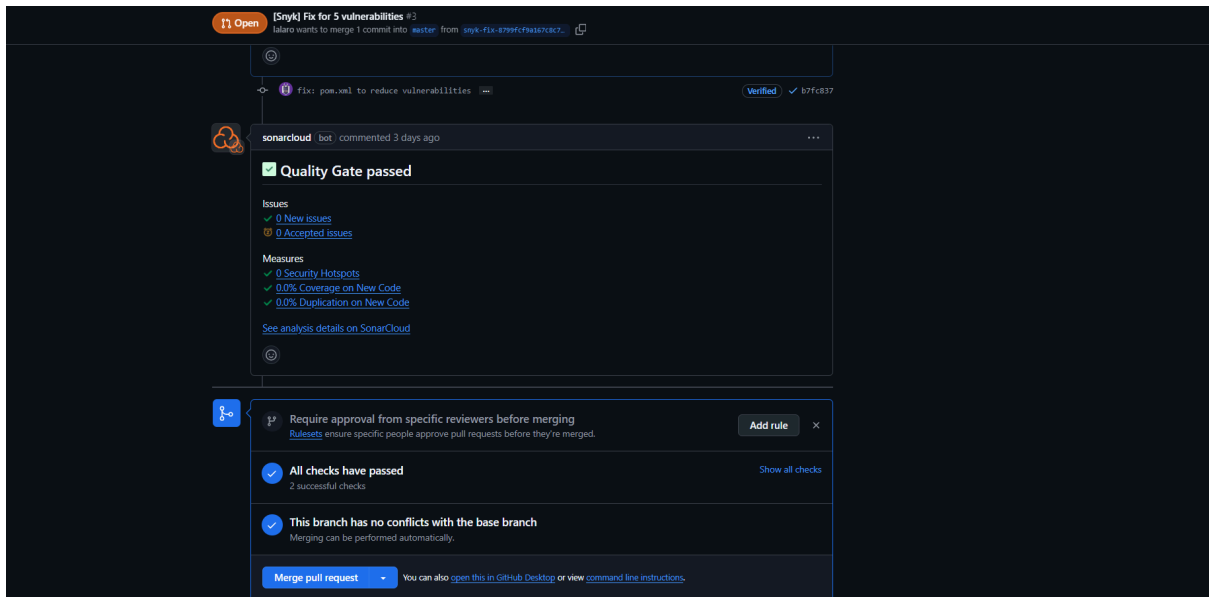
Unsubscribe

Customize

You're receiving notifications because you authored the thread.

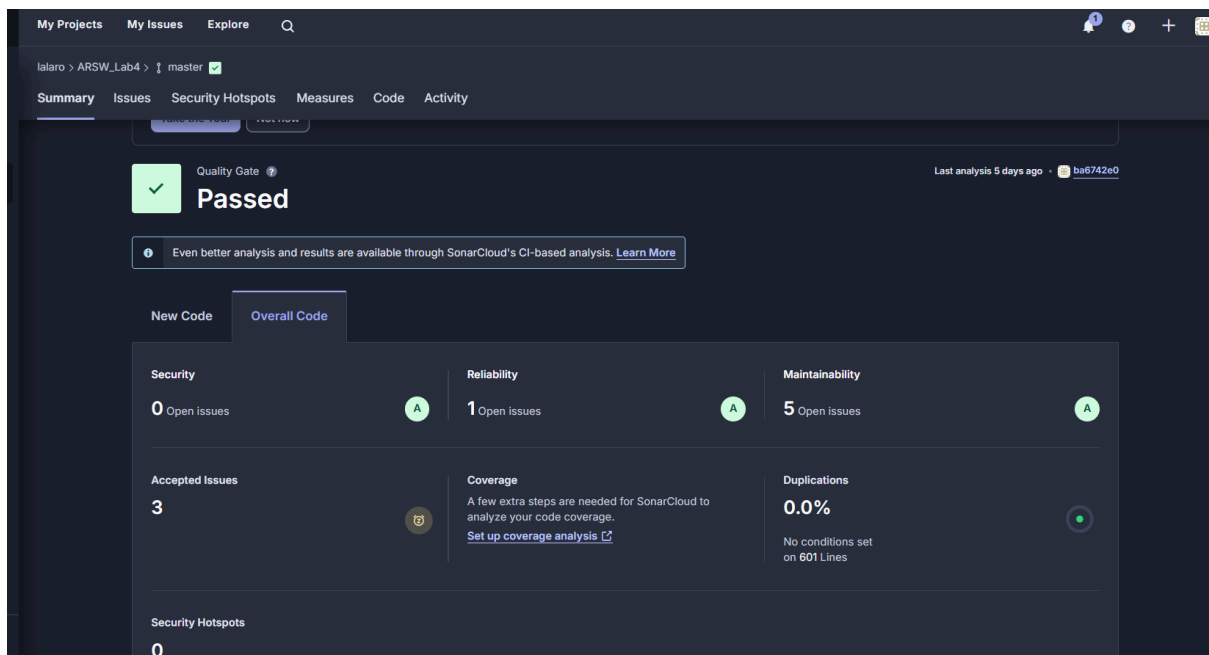
2 participants

Lock conversation



- Corrija todos los hallazgos informados.

De esta forma y solo con el PR realizado por snyk se resolvieron 3 vulnerabilidades



The screenshot shows the SonarCloud web interface for project ARSW_Lab4. The left sidebar contains navigation links: Overview, Main Branch, Pull Requests (3), Branches (1), Information, and Administration. The main area displays a 'Filters' panel on the left with categories like Clean Code Attribute, Software Quality, and Severity. The central panel shows a list of issues with details such as the issue type (e.g., Intentionality, Consistency), description, severity (e.g., Minor, Major), and effort (e.g., 2min effort, 7 years ago).

- El proceso de remediación

1.

This screenshot shows a detailed view of issues in SonarCloud. At the top, there's a 'Bulk Change' button and navigation controls. Below, a list of issues is displayed for the file `src/.../eci/arsw/blueprints/services/BlueprintsServices.java`. Each issue entry includes a checkbox, the issue type (Consistency), a description (e.g., 'Remove this field injection and use constructor injection instead.'), and metadata like severity (Major) and effort (5min effort, 7 y). The bottom of the list indicates '2 of 2 shown'.

```
@Service
public class BlueprintsServices {

    BlueprintsPersistence bpp;
    BlueprintsFilter filter;

    @Autowired
    public BlueprintsServices(BlueprintsPersistence bpp, BlueprintsFilter filter) {
        this.bpp = bpp;
        this.filter = filter;
    }
}
```

2.

sonarcloud

My Projects My Issues Explore Q

ARSW_Lab4

Overview

Main Branch

Pull Requests 0

Branches 1

Information

Administration

Collapse

lalaro > ARSW_Lab4 > master

Summary Issues Security Hotspots Measures Code Activity

2 / 8 Issues

src/.../BlueprintsPersistence.java

Provide the parametrized type for this generic.

src/.../impl/Tuple.java

Replace this if-then-else statement by a single return statement.

src/.../services/BlueprintsServices.java

Remove this field injection and use constructor injection instead.

Remove this field injection and use constructor injection instead.

The return type of this method should be an interface such as "List" rather than the implementation "ArrayList".

src/.../ui/Main.java

Move the array designators [] to the type.

Replace this use of System.out by a logger.

Where Why Activity

Open in IDE

```

27     hash = 17 * hash + Objects.hashCode(this.o1);
28     hash = 17 * hash + Objects.hashCode(this.o2);
29     return hash;
30 }
31
32 @Override
33 public boolean equals(Object obj) {
34     if (this == obj) {
35         return true;
36     }
37     if (obj == null) {
38         return false;
39     }
40     if (getClass() != obj.getClass()) {
41         return false;
42     }
43     final Tuple<?, ?> other = (Tuple<?, ?>) obj;
44     if (!Objects.equals(this.o1, other.o1)) {
45         return false;
46     }
47     if (!Objects.equals(this.o2, other.o2)) {
48         return false;
49     }
50     return true;
51 }
52
53
54
55

```

Replace this if-then-else statement by a single return statement.

© 2018-2024 SonarSource SA. All rights reserved. Terms Pricing Privacy Cookie Policy Security Community Documentation Contact us Status About

```

@Override
public boolean equals(Object obj) {
    if (this == obj) {
        return true;
    }
    if (obj == null) {
        return false;
    }
    if (getClass() != obj.getClass()) {
        return false;
    }
    final Tuple<?, ?> other = (Tuple<?, ?>) obj;
    return Objects.equals(this.o1, other.o1) && Objects.equals(this.o2, other.o2);
}

```

3.

```

1  juan.f... package edu.eci.arsw.blueprints.ui;
2
3  juan.f... import edu.eci.arsw.blueprints.persistence.BlueprintNotFoundException;
4  juan.f... import edu.eci.arsw.blueprints.services.BlueprintsServices;
5          import org.springframework.context.ApplicationContext;
6          import org.springframework.context.support.ClassPathXmlApplicationContext;
7
8          public class Main {
9
10         juan.f... public static void main(String a[]) throws BlueprintNotFoundException {
11         juan.f...     ApplicationContext ac = new ClassPathXmlApplicationContext("applicationContext.xml");
12         juanpa...     BlueprintsServices gc = ac.getBean(BlueprintsServices.class);
13         System.out.println(gc.getBlueprintsByAuthor("_authorname_"));
14
15         }
16     }

```

Replace this use of System.out by a logger.

```

1 package edu.eci.arsw.blueprints.ui;
2
3 import java.util.logging.Logger;
4 import edu.eci.arsw.blueprints.persistence.BlueprintNotFoundException;
5 import edu.eci.arsw.blueprints.services.BlueprintsServices;
6 import org.springframework.context.ApplicationContext;
7 import org.springframework.context.support.ClassPathXmlApplicationContext;
8
9 public class Main {
10
11     Logger logger = Logger.getLogger(getClass().getName());
12
13     Run | Debug
14     public static void main(String[] arStrings) throws BlueprintNotFoundException {
15         ApplicationContext ac = new ClassPathXmlApplicationContext(configLocation:"applicationContext.xml");
16         BlueprintsServices gc = ac.getBean(name:BlueprintsServices.class);
17     }
18
19     public void doSomething() {
20         logger.info(gc.getBlueprintsByAuthor("_authorname_"));
21     }
22 }

```

4.

src/.../arsw/blueprints/persistence/impl/BlueprintFiltersTest.java [See all issues](#)

Move this file to a named package.

```

1 100946... import edu.eci.arsw.blueprints.filters.RedundancyFilter;
2 import edu.eci.arsw.blueprints.filters.SubsamplingFilter;
3 import edu.eci.arsw.blueprints.model.Blueprint;
4 import edu.eci.arsw.blueprints.model.Point;
5 import org.junit.Test;
6 import static org.junit.Assert.*;
7
8 public class BlueprintFiltersTest {
9
10     @Test
11     public void testRedundancyFilter() {
12         Point[] points = new Point[]{
13             new Point(0, 0), new Point(0, 0),
14             new Point(10, 10), new Point(10, 10)
15         };
16         Blueprint bp = new Blueprint("author1", "blueprint1", points);
17     }

```

BlueprintsServices.java 1 | BlueprintFiltersTest.java 1 X | Extension: Extension Pack for Java | BlueprintsPersiste

```

src > test > java > edu > eci > arsw > blueprints > persistence > impl > BlueprintFiltersTest.java > BlueprintFiltersTest
1 package edu.eci.arsw.blueprints.test.persistence.impl;
2
3 import edu.eci.arsw.blueprints.filters.RedundancyFilter;
4 import edu.eci.arsw.blueprints.filters.SubsamplingFilter;
5 import edu.eci.arsw.blueprints.model.Blueprint;
6 import edu.eci.arsw.blueprints.model.Point;
7 import org.junit.Test;
8 import static org.junit.Assert.*;
9
10 public class BlueprintFiltersTest {
11

```

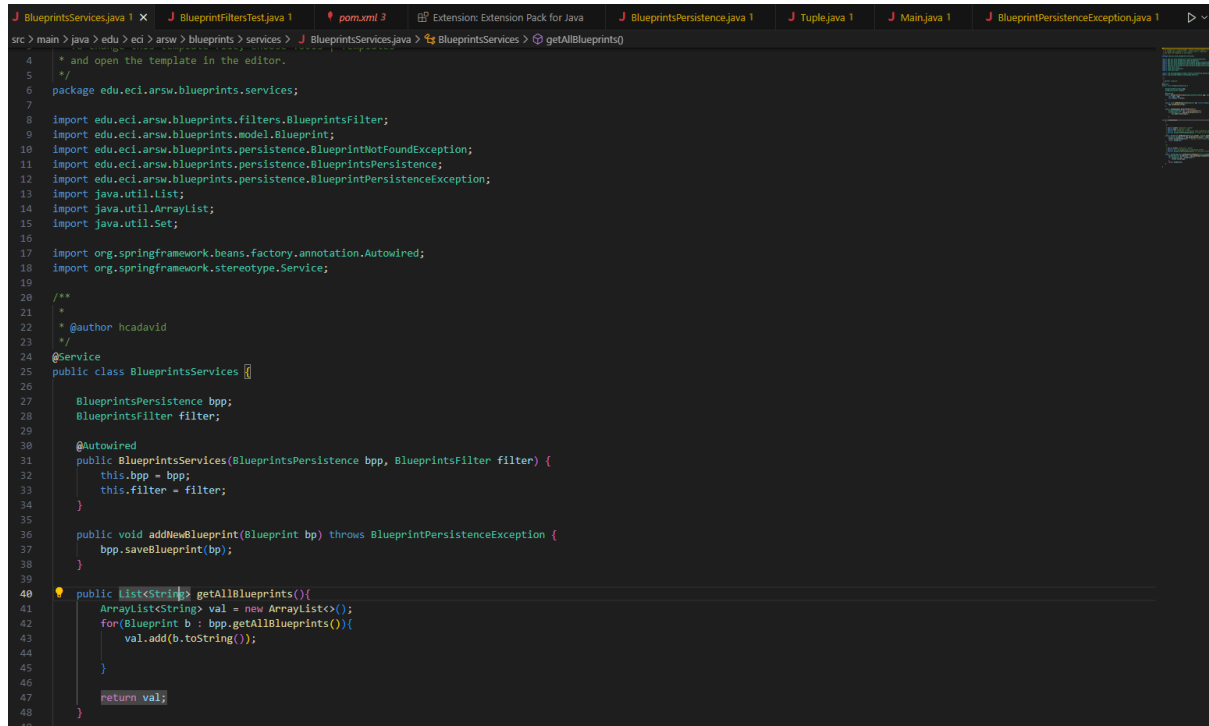
5.

```
}
```

```
public ArrayList<String> getAllBlueprints(){
```

The return type of this method should be an interface such as "List" rather than the implementation "ArrayList".

```
ArrayList<String> val = new ArrayList<>();  
for(Blueprint b : bpp.getAllBlueprints()){  
    val.add(b.toString());  
}  
  
return val;  
}
```

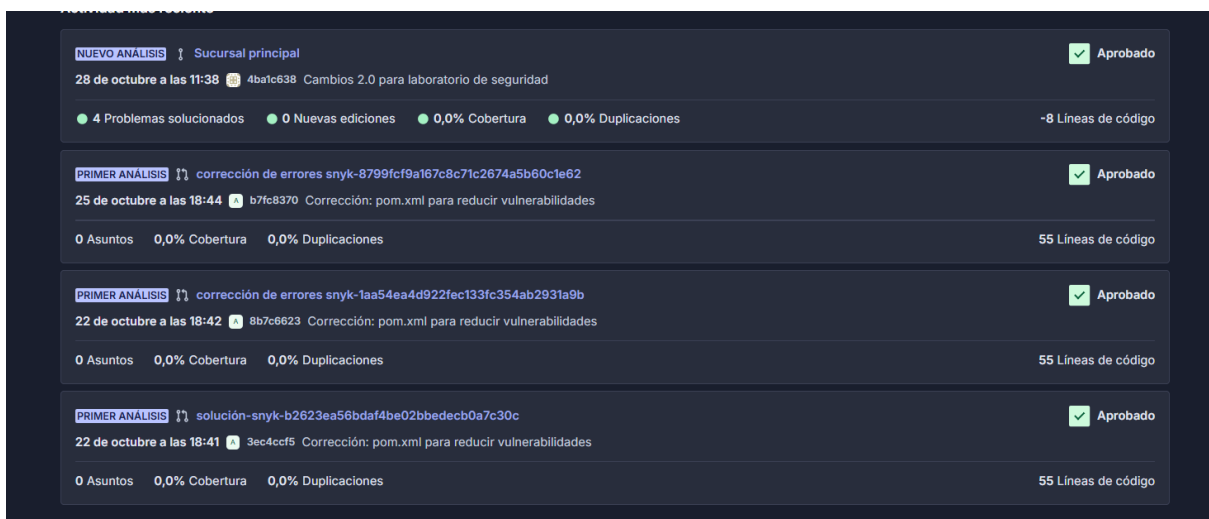
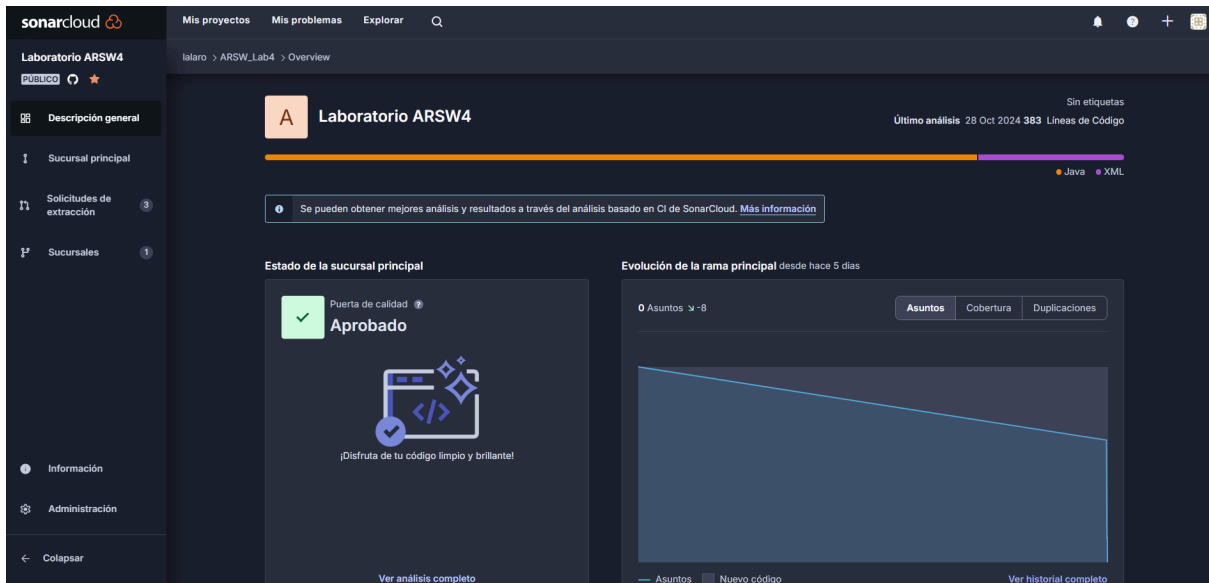


```
J BlueprintServices.java 1 x J BlueprintFiltersTest.java 1 pom.xml 3 Extension: Extension Pack for Java J BlueprintsPersistence.java 1 J Tuple.java 1 J Main.java 1 J BlueprintPersistenceException.java 1  
src > main > java > edu > eci > arsw > blueprints > services > J BlueprintServices.java > BlueprintServices > getAllBlueprints()  
4  * and open the template in the editor.  
5  */  
6  package edu.eci.arsw.blueprints.services;  
7  
8  import edu.eci.arsw.blueprints.filters.BlueprintsFilter;  
9  import edu.eci.arsw.blueprints.model.Blueprint;  
10 import edu.eci.arsw.blueprints.persistence.BlueprintNotFoundException;  
11 import edu.eci.arsw.blueprints.persistence.BlueprintsPersistence;  
12 import edu.eci.arsw.blueprints.persistence.BlueprintPersistenceException;  
13 import java.util.List;  
14 import java.util.ArrayList;  
15 import java.util.Set;  
16  
17 import org.springframework.beans.factory.annotation.Autowired;  
18 import org.springframework.stereotype.Service;  
19  
20 /**  
21  *  
22  * @author hcadavid  
23  */  
24 @Service  
25 public class BlueprintsServices {  
26  
27     BlueprintsPersistence bpp;  
28     BlueprintsFilter filter;  
29  
30     @Autowired  
31     public BlueprintsServices(BlueprintsPersistence bpp, BlueprintsFilter filter) {  
32         this.bpp = bpp;  
33         this.filter = filter;  
34     }  
35  
36     public void addNewBlueprint(Blueprint bp) throws BlueprintPersistenceException {  
37         bpp.saveBlueprint(bp);  
38     }  
39  
40     public List<String> getAllBlueprints(){  
41         ArrayList<String> val = new ArrayList<>();  
42         for(Blueprint b : bpp.getAllBlueprints()){  
43             val.add(b.toString());  
44         }  
45     }  
46  
47     return val;  
48 }  
49
```

- Las métricas posteriores a la remediación.

Al final después de realizar los cambios sugeridos por el sonarCloud podemos ver como cada uno de los issue, excepto por uno que se genero después de los cambios y posteriormente fue solucionado.

Para terminar se muestra la gráfica de sonarCloud sin errores o vulnerabilidades en el proyecto y con 8 issue solucionados.



Después de hacer el pr aun quedo un problema por solucionar:



lalaro > ARSW_Lab4 > master

Summary Issues Security Hotspots Measures Code Activity

5 / 5 issues

src/.../impl/Tuple.java

Replace this if-then-else statement by a single return statement.

src/.../services/BlueprintsServices.java

Remove this field injection and use constructor injection instead.

The return type of this method should be an interface such as "List" rather than the implementation "ArrayList".

src/.../ui/Main.java

Move the array designators [] to the type.

src/.../impl/BlueprintFiltersTest.java

Move this file to a named package.

5 of 5 shown

Adaptability | Not modular

Move this file to a named package.

The default unnamed package should not be used [java:S1220](#)

Software qualities impacted: **Maintainability**

Confirmed Not assigned Code Smell Minor

Where is the issue? Why is this an issue? How can I fix it? Activity More info

Open in IDE

src/.../arsw/blueprints/persistence/impl/BlueprintFiltersTest.java

See all issues in this file

```
1 100946...
2 import edu.eci.arsw.blueprints.filters.RedundancyFilter;
3 import edu.eci.arsw.blueprints.filters.SubsamplingFilter;
4 import edu.eci.arsw.blueprints.model.Blueprint;
5 import edu.eci.arsw.blueprints.model.Point;
6 import org.junit.Test;
7 import static org.junit.Assert.*;
8
9 public class BlueprintFiltersTest {
10
11     @Test
12     public void testRedundancyFilter() {
13         Point[] points = new Point[] {
14             new Point(0, 0), new Point(0, 0),
15             new Point(10, 10), new Point(10, 10)
16         };
17     }
18 }
```

⌵ Tuple.java ⌵ BlueprintsServices.java × ⌵ BlueprintsPersistence.java ⌵ Main.java ⌵ RedundancyFilter.java ⌵ BlueprintFiltersTest.java

```
1 package edu.eci.arsw.blueprints.services;
2
3 import edu.eci.arsw.blueprints.filters.BlueprintsFilter;
4 import edu.eci.arsw.blueprints.model.Blueprint;
5 import edu.eci.arsw.blueprints.persistence.BlueprintNotFoundException;
6 import edu.eci.arsw.blueprints.persistence.BlueprintsPersistence;
7 import edu.eci.arsw.blueprints.persistence.BlueprintPersistenceException;
8 import java.util.ArrayList;
9 import java.util.List;
10 import java.util.Set;
11 import org.springframework.beans.factory.annotation.Autowired;
12 import org.springframework.stereotype.Service;
13
14 /**
15  *
16  * @author hcadavid
17  */
18 @Service
19 public class BlueprintsServices {
20
21     private final BlueprintsPersistence bpp;
22     private final BlueprintsFilter filter;
23
24     @Autowired
25     public BlueprintsServices(BlueprintsPersistence bpp, BlueprintsFilter filter) {
26         this.bpp = bpp;
27         this.filter = filter;
28     }
29
30     public void addNewBlueprint(Blueprint bp) throws BlueprintPersistenceException {
31         bpp.saveBlueprint(bp);
32     }
33 }
```